In the claims:

1. (currently amended) A method of securing packet data transferred between [[a pair]] non-overlapping pairs of stations of a group of more than two stations on a backbone, the backbone comprising an ingress point and egress point, the method comprising the steps of:

receiving a first packet at the ingress point of the backbone from [[any]] a sending first station of the group of stations, the packet including an original header with a source IP address of the sending station and a destination IP address of a receiving second station of the group of stations;

receiving a second packet at the ingress point of the backbone from a sending third station of the group of stations, the packet including an original header with a source IP address of the sending station and a destination IP address of a receiving fourth station of the group of stations;

wherein the first packet is associated with a first point-to-point communication, the second packet is associated with a second point-to-point communication, and the first communication is unrelated to the second communication except that the first, second, third and fourth stations belong to the group of stations;

transforming, at the ingress point of the backbone, the first packet by adding a group header including a group identifier corresponding to the group of stations and a destination address for the first packet;

transforming, at the ingress point of the backbone, the second packet by adding a group header including the group identifier corresponding to the group of stations and a destination address for the second packet;

transforming, at the ingress point of the backbone, both the [[packet]] first packet and the second packet according to the group security association associated with the group identifier, wherein the ingress point is a provider edge device;

forwarding the transformed [[packet]] first and second packets over the backbone to the egress point using the group identifier as a backbone address;

receiving, at the egress point in the backbone, the transformed [[packet]] first and second packets;

restoring, at the egress point in the backbone, both the first transformed packet and the second transformed packet according to the group security association associated with the group identifier;

transforming, at the egress point in the backbone, the first and second restored [[packet]] packets by removing the respective group [[header]] headers;

forwarding the first restored transformed packet to the receiving second station,

and

forwarding the second restored transformed packet to the receiving fourth station,

whereby the same security association is used for unrelated communications between [[any pair]] non-overlapping pairs of stations of the group of stations.

2. (previously presented) The method according to claim 1, wherein the step of transforming at the ingress point of the backbone includes the step of retaining fields of the packet needed to transfer the packet to the destination address of the receiving station from the egress point.

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (currently amended) A network architecture for providing secure point-to-point communication between ~~at least two~~ non-overlapping pairs of members of a private network

including more than two members over a communication link, the network architecture comprising:

[[a]] first and third sending stations [[station]] which are ~~is any one of the more than two~~ members of the private network;

an ingress point to the communication link;

an egress point from the communication link;

[[a]] second and fourth receiving stations [[station]], coupled to the egress point;

the ingress point functioning to:

receive a first packet from the first station, the first packet including an original header with a source IP address of the first station and a destination IP address of the second station;

receive a second packet from the third station, the second packet including an original header with a source IP address of the third station and a destination IP address of the fourth station;

transform the first and second packets [[packet]] by adding a group header including a group identifier corresponding to the group of stations and a common destination address for both the first and second packets ~~the packet~~;

transform both the first and second packets [[packet]] according to the group security association associated with the group identifier; and

forward the transformed first and second packets [[packet]] over the backbone to the egress point using the group identifier as a backbone address;

the egress point functioning to:

receive the transformed first and second packets [[packet]];

restore the transformed first and second packets [[packet]] according to the group security association associated with the group identifier;

transform the restored first and second packets [[packet]] by removing the respective group headers [[header]];

forward the restored transformed first packet to the receiving second station,

and

forward the restored transformed second packet to the receiving fourth station, wherein the first packet is associated with a first point-to-point communication, the second packet is associated with a second point-to-point communication, and the first communication is unrelated to the second communication except that the first, second, third and fourth stations belong to the group of stations,

whereby the same security association is used for distinct communications between [[any pair]] non-overlapping pairs of stations of the group of stations.

11. (cancelled)

12. (original) The network architecture of claim 10, wherein the communication link comprises a plurality of provider devices, and wherein the egress point is one of the plurality of provider devices.

13. (original) The network architecture of claim 10, wherein the group comprises at least three stations.

14. (cancelled)

15. (cancelled)

16. (original) The network architecture according to claim 10 wherein the means for securing data includes transform logic for encrypting only a portion of data transferred between the ingress point and egress point of the communication link.